“ATAQUES CIBERNÉTICOS” (“CYBER ATTACKS”)

Profesor:

CORONEL JAIRO CACERES

Trabajo presentado por:

ALEXANDER OLAYA OLIVEROS [1]

UNIVERSIDAD MILITAR NUEVA GRANADA

FACULTAD DE RELACIONES INTERNACIONALES, ESTRATEGIA Y SEGURIDAD

ESPECIALIZACIÓN EN ADMINISTRACIÓN DE LA SEGURIDAD

BOGOTA D.C., JUNIO DE 2021

---

1 Profesional en Administración de Empresas y estudiante de la Especialización en Administración de la Seguridad de la Universidad Militar Nueva Granada, Bogotá, Colombia.
Correo: alexanderolaya42@gmail.com CÓDIGO ORCID https://orcid.org/0000-0002-6957-0736

Resumen

Los inconvenientes que representa el ataque cibernético "*cyber attack*" se basan en la dificultad para detectarlos y detectar los bandos en contienda, dado que al hacerlo se pueden generar ataques contra las personas (ciudadanos), empresas o corporaciones, etc. Por eso, los ataques cibernéticos se constituyen como un asunto global dado que el ecosistema digital y la protección de este frente a diferentes acciones ilegales, son asuntos que atañen a todos los países (sin fronteras claras). Por esto, a lo largo de este ensayo se pondrán en evidencia diferentes tipos de ataque cibernético, así como el futuro y presente del mismo.

Palabras claves: Ataque cibernético, cibercrimen, delitos informáticos, amenaza.

Abstract

The drawbacks that the cyber attack "ataques cibernéticos" represents are based on the difficulty of detecting them and detecting the contending sides, since doing so can generate attacks against people (citizens), companies or corporations, etc. Cyber attacks are constituted as a global issue since the digital ecosystem and its protection against different illegal actions, are matters that concern all countries (without clear borders). For this reason, throughout this essay different types of cyber attack will be highlighted, as well as its future and present.

Key words: Cyber attack, Cybercrime, informatic felonies, threat.

Introducción

La dinámica del Cibercrimen y su constante evolución exponencial ha propiciado que delincuentes que hasta hace poco actuaban de manera aislada, sin coordinación, con un alcance local, en la actualidad constituyan organizaciones trasnacionales complejas de Cibercrimen.

El Cibercrimen forma parte ya de la realidad criminológica de nuestro mundo, pero en muchas ocasiones se exagera la amenaza que el mismo supone y en otras no se percibe el riesgo real al que el uso de las TIC conlleva. La lógica de que esta «novedad» dure tanto, es la revolución de las TIC (como en el caso de las redes sociales, las cuales se constituyen como un área de interés esencial para las diferentes aplicaciones de ciberseguridad), como concepto amplio, abierto y dinámico que engloba todos los elementos y sistemas utilizados en la actualidad para el tratamiento de la información, su intercambio y comunicación en la sociedad actual, en la que se enmarca el fenómeno del Cibercrimen. No ha terminado todavía, ni lo hará en mucho tiempo, lo que supone que la cibercriminalidad o delincuencia asociada al ciberespacio seguirá expandiéndose y evolucionando en las próximas décadas (Amato, et al., 2018).

Para comprender la problemática del cibercrimen, es necesario conocer la forma de actuar de un criminal informático y, por lo tanto, no se debe confiar en todo lo que brinda el internet dado que los intrusos pueden engañar a sus víctimas con publicidades falsas o sitios web que pueden dirigir a páginas no oficiales y que no son auténticas, ataques de *malware* o robos de información.

Adicionalmente, se deben conocer las leyes que pueden proteger y brindar apoyo a las víctimas de estos delitos ya que penalizan las acciones incorrectas de los delincuentes informáticos. Actualmente existen muchas vulnerabilidades que afectan la información y que

han aumentado cada año, dado que a medida que avanza la tecnología los intrusos también encuentran nuevas formas y mediospara afectar, modificar o ingresar a la información confidencial (González, 2020).

El cibercrimen es una problemática a nivel mundial y es un tema bastante amplio, por eso, se debe conocer su caracterización, así como los ataques más comunes a nivel nacional con el fin de comprender la importancia de la formación de cultura informática segura para los empleados de cualquier organización y de esta manera minimizar los riesgos.

Planteamiento del problema

A medida que los sistemas informáticos y la tecnología evolucionan, son más indispensables para la sociedad, ya que los usuarios centran sus actividades en estos medios y les facilita la realización de diferentes funciones; sin embargo, existen problemas de seguridad que se han evidenciado por que los intrusos aprovechan la confianza, el descuido o falta de conocimiento de los usuarios para lograr obtener información confidencial o ingresar a los sistemas que los usuarios utilizan.

Esencialmente, existe una gran problemática en cuanto a los riesgos que se enfrentan las empresas, por lo tanto, es importante implementar los controles necesarios para asumir un ataque de un ciberdelincuente.

El cibercrimen es en la actualidad uno de los delitos más perseguidos por la policía, con la aparición de internet los delitos informáticos han representado un riesgo que va en contra de la privacidad de las personas desde suplantación de identidad hasta robar completamente su información, lo cual genera pérdidas para grandes y pequeñas empresas hasta personas comunes que manejan datos importantes desde sus hogares, pueden llegar a ser víctimas de estos delitos por falta de herramientas y conocimiento en seguridad.

Entre los delitos más frecuentes utilizados por los ciberdelincuentes están las estafas, phishing y la suplantación de identidad además del ransomware que es uno de los malware más reconocidos por encriptar la información de sus víctimas y extorsionarlos si desean recuperar sus datos de lo contrario son eliminados.

En torno a la problemática del cibercrimen existen dos campos que lo abordan el primero es: el derecho referente al delito que se cometió y que debe ser sancionado, este es un ámbito

bastante amplio, ya que aún existen estudios para determinar qué acciones pueden ser consideradas delito informático y el campo de seguridad informática se refiere a las herramientas, técnicas y prácticas en cuanto a conceptos técnicos y preventivos que se deben tener en cuenta para minimizar los riesgos, se centra en la protección de los sistemas tanto para software como hardware, vulnerabilidades en programas, problemas de seguridad e incidentes informáticos de todo tipo.

En efecto, el cibercrimen es un problema constante que afecta la privacidad y trae grandes pérdidas a los diferentes sectores de las empresas. Colombia es uno de los países más afectados, las denuncias más frecuentes son por fraudes bancarios, compra de productos o suplantación de identidad.

Ahora bien, existe una alternativa que favorece a las víctimas de los delitos informáticos, en donde se penalizan acciones inadecuadas con respecto a la violación de la privacidad de las personas en el mundo cibernético, en Colombia se han creado leyes y normas que sancionan los actos que no son permitidos en el entorno informático, de manera que puedan regular las acciones de los criminales, debido al uso inadecuado de los medios tecnológicos (González, 2020).

Formulación del problema

Es importante analizar los delitos informáticos más frecuentes en Colombia, algunos casos reales que han afectado a diferentes organizaciones, así como a los usuarios, las sanciones que pueden recibir los ciberdelincuentes y las recomendaciones para minimizar los riesgos. Es importante tener en cuenta las nuevas técnicas que utilizan los ciberdelincuentes e informar a las empresas de los riesgos más frecuentes para que puedan optar por las mejores alternativas para contrarrestar los ataques, ya que les ayudará a diseñar planes de contingencia que minimicen el impacto que puede causar la pérdida de información o el daño de los sistemas.

Con base en el planteamiento anterior, se llega a generar el siguiente interrogante: ¿Cómo afecta el cibercrimen a las empresas de Colombia y como minimizar los riesgos?

En realidad, los delitos informáticos se incrementan en la misma medida que evoluciona la tecnología, las víctimas pueden llegar a ser usuarios comunes que realizan tareas básicas, que por falta de conocimiento reciben un ataque o grandes empresas con información confidencial son vulnerables a los fraudes, virus informáticos, o cualquier tipo de delito que se encuentre en la red, lo cual puede causarles grandes pérdidas.

Por lo anterior, es necesario que Colombia se compare con otros países para analizar esta problemática y que sea una de las prioridades combatir la delincuencia informática, ya que existen amenazas informáticas no solo en Colombia sino a nivel mundial. Se debe iniciar con cada persona, utilizando los medios tecnológicos correctamente puede aportar a la seguridad si tiene el conocimiento necesario y lo práctica, implementando en sus actividades diarias simples normas de seguridad hasta utilizar herramientas más avanzadas que le ayuden a

mitigar los riesgos.

En las empresas la información se considera como uno de los activos más importantes, por tal razón es el principal objetivo para los ciberdelincuentes y la manera de obtenerla cada día es más novedosa, los delincuentes informáticos buscan nuevas maneras de conseguir la información sin ser reconocidos, pueden manipularla fácilmente atentando contra la privacidad de las personas tanto física como moral. Si bien es cierto que la responsabilidad de la seguridad de la información es de los usuarios, las empresas deben concientizar a sus empleados, utilizar mecanismos e invertir lo necesario en los servicios de las tecnologías de la información y las herramientas para protegerlos, garantizando la confiabilidad, disponibilidad e integridad a sus clientes, empleados y las actividades que realizan.

Por esto, las empresas deben controlar la privacidad de la información y su seguridad depende de las mismas, es necesario que inviertan en la protección de los datos y no subestimen los gastos, esto puede ser mínimo comparado con las pérdidas que les puede generar cualquier delito informático en el momento de no tener disponible la información, principalmente se debe reconocer que es una realidad que afecta a cualquier empresa, aunque no se puede tener un sistema completamente seguro es necesario implementar herramientas y mecanismos de seguridad para reducir riesgos (González, 2020).

Marco conceptual

Ataques más comunes en el ciberespacio colombiano

Es importante conocer los ataques más comunes que se presentan y su origen. Estos ataques pueden afectar a empresas, usuarios comunes, hasta estados y sociedades, es una de las amenazas más significativas para el mundo. Por lo tanto, se debe priorizar la seguridad en este entorno sobre todo cuando las actividades que se realizan y la información que se utiliza dependen del uso de la red y los sistemas informáticos.

De acuerdo con la información de la revista portafolio en el año 2018 (como se cita en González, 2020), según investigaciones de la compañía tecnológica Microsoft, Colombia se encontraba en el segundo país de América Latina más expuesto a riesgos de delitos informáticos. En la investigación de la revista portafolio además se encontró que en Colombia el 12% de sistemas móviles han sido atacados por malware.

Según la revista Semana en un artículo publicado en 2019 (como se cita en González, 2020), de acuerdo con un estudio realizado a 60 países, Argelia obtuvo el primer puesto con respecto a problemas de seguridad informática y Colombia ocupaba el puesto 39, es decir para el año 2019 la seguridad en Colombia era regular.

A continuación, se definen los diferentes ataques más comunes en el ciberespacio colombiano y temas relevantes del cibercrimen:

Ataques bancarios. Los intrusos centran su atención en las entidades bancarias, ya que obtienen beneficios lucrativos, además pueden obtener información privada que los beneficia. A pesar de que las empresas utilizan mecanismos de seguridad los intrusos emplean técnicas para engañar a sus víctimas como: ingeniería social o ataques de

malware. Según un informe de ataques dirigidos al sector financieros en Colombia y América Latina, aproximadamente al mes un banco podría recibir hasta 10 ataques cibernéticos en su infraestructura y los daños causados a estas empresas podrían estar entre 97.000 a 268.000 millones de dólares anuales (como se cita en González, 2020). Por esta razón se está considerando brindar un seguro por riesgo cibernético.

Cibercrimen. Se refiere a conductas inadecuadas consideradas como delitos realizados en el ciberespacio. Entre estos podemos encontrar suplantación de identidad, robo de información, fraudes, estafas entre otros. No solo afectan la privacidad y la economía, también perjudican la integridad de las personas víctimas de estos delitos. De acuerdo con *Digiware* (como se cita en González, 2020), en Colombia existen casos de fraudes a través de correos electrónicos realizados a entidades financieras con un 39%, telecomunicaciones 25%, gobierno 15% industria 9%, sector energético 3%, correspondientes a ataques diarios. Las denuncias más frecuentes han sido por transacciones bancarias, compra de productos o suplantación de identidad. Para evitar este tipo de delitos se recomienda a los usuarios no realizar transacciones con colaboración de otras personas, cuando se presenta inconvenientes dirigirse directamente a la entidad bancaria, no ingresar a los links que llegan a los correos electrónicos aparentemente emitidos de las entidades.

Ciberespacio. Es un entorno no físico creado por equipos computacionales unidos para interoperar en una red, las personas que se conectan a estos equipos pueden interactuar como en el mundo real sin estar presentes físicamente, además las personas pueden comprar en línea, compartir información, explorar entre otros.

Estafas electrónicas. Es uno de los delitos más comunes en Colombia. El uso de redes

sociales acompañadas del mundo digital permite que los intrusos obtengan sus beneficios, desafortunadamente muchas de las víctimas por miedo no denuncian. La delegada de la seguridad Ciudadana de la fiscalía General Claudia Carrasquilla manifestó “que el aumento del delito de estafas electrónicas está relacionado con la facilidad que tienen los delincuentes informáticos para acceder a la información de sus víctimas, ya que se confían de páginas que aparecen sin comprobar la autenticidad de esta, ni de los productos ofrecidos. Un caso de este tipo fue judicializado por la Fiscalía cuando fueron capturadas 8 personas de una organización que a través de internet ofrecían servicios para organizar eventos sociales como bodas y citaba a los interesados a reuniones para conocer los descuentos, donde solicitaban un adelanto para los detalles de la fiesta la cual no se realizaba. Los estafadores aproximadamente recibieron alrededor de 240 millones de pesos entre febrero de 2017 a noviembre del 2018, por 35 supuestos eventos (como se cita en González, 2020).

Impacto del cibercrimen. Cuando se menciona noticias sobre cibercrimen las personas erróneamente suelen pensar que estos incidentes se presentan a grandes empresas y que su compañía no recibiría un ataque, sin embargo, los delitos informáticos son una de las principales amenazas que afecta a la economía mundial. Interpol informa que solo en Europa las pérdidas generadas por el cibercrimen aproximadamente llegan a los 750.000 millones de euros, lo cual significa que el impacto del cibercrimen afecta considerablemente la economía nacional y local (como se cita en González, 2020).

En el año 2017, la BBC reportó que “numerosas compañías y entes gubernamentales en todo el mundo reportaron que fueron blanco de un ataque cibernético de gran escala”. En el presente año 2020 con el aumento del uso de la tecnología tanto para empresas como

usuarios comunes se considera que poco a poco las contraseñas podrían desaparecer, se debe tener en cuenta el estudio de la inteligencia artificial y la protección colaborativa deberá ser implementada. Los delitos informáticos perjudican a las empresas con pérdidas de aproximadamente 1 billón de dólares anuales tres veces más que los costos por desastres naturales. Es necesario para las empresas contar con especialistas en seguridad de la información ya que se debe detectar a tiempo los problemas de seguridad que existen en las empresas y que dejan en riesgo la información, ya que al afectar uno de los pilares que la hacen segura como la confidencialidad, integridad o disponibilidad afecta las actividades normales de la empresa y puede generar pérdidas, teniendo en cuenta este panorama las empresas deben utilizar los recursos tecnológicos a su favor y protegerse (BBC, 2017).

Malware. Son programas maliciosos, cuyo fin es dañar dispositivos y robar datos con algún fin lucrativo. Algunos de ellos son virus, troyanos, *spyware*, gusanos, *ransomware* entre otros. Actualmente se están presentando ataques de malware aprovechando las campañas o información sobre coronavirus, según informes de Nokia, Microsoft y agencias de seguridad los más comunes son:

Troyano coronavirus. Este se dirige a usuarios de Windows presenta un mapa de casos de coronavirus por ciudades y regiones en tiempo real, una vez el usuario ingresa descarga un software maligno, el cual obtiene credenciales de usuario y datos personales.

Otro caso de malware. Se refiere a una aplicación para los sistemas Android que supuestamente informa la ubicación de personas cercanas con COVID-19 y rastrear su propagación, pero se trata de un *ransomware*, el verdadero objetivo de esta aplicación

es bloquear el dispositivo y solicitar rescate para recuperar su funcionamiento.

Phishing. Se refiere al método utilizado por ciberdelincuentes para engañar a sus víctimas solicitando información confidencial como contraseñas, a través de correos electrónicos o páginas web falsas. Existen varios casos de phishing uno de estos se presentó en el año 2016 en el cual los seguidores de James Rodríguez, fueron víctimas de un ciberdelincuente quien solicitaba datos personales, les hizo creer que se comunicaban con el futbolista y ellos proporcionaron información confidencial como claves de correo. El ciberdelincuente fue reconocido y condenado a 4 años de prisión.

Ransomware. Los intrusos obtienen información para luego solicitar un rescate. Colombia presentaba el mayor ataque de malware en el 2018, según un informe realizado por la compañía de ciberseguridad Eset (como se cita en González, 2020). Según el informe mencionado en el 2018 Colombia presentaba el 30% de los casos estudiados, Perú el 16%, México 14%, Brasil 11% y Argentina 9%. En este tipo de ataque se encuentran SamSam que controla remotamente el equipo y Crysis que puede introducirse a través de correos o redes sociales (Valle, 2016).

Riesgos del cibercrimen. actualmente la mayoría de las actividades que realizan las personas están relacionadas con el mundo cibernético, a pesar de las ventajas que se puede encontrar en la red, también es utilizado con fines negativos, los ataques que se presentan en el ciberespacio son un reto para las empresas, ya que pueden afectar las funciones y finanzas, donde la información podría ser modificada, robada, o eliminada, por lo tanto cuando se identifica un riesgo en una empresa es necesario buscar la vulnerabilidad y aplicar las medidas de seguridad necesarias para evitar el desarrollo de un ataque. La falta de conocimiento sobre los riesgos que se encuentran en la red es la

principal causa de los problemas informáticos, las personas ignoran muchas de las advertencias y amenazas y no comprenden los alcances de un ciberdelincuente por lo tanto siguen realizando conductas que los convierte en víctimas de los ataques. Las empresas son responsables de la seguridad de los datos y de la privacidad que debe tener el manejo de la información de los clientes, por lo tanto, las empresas deben conocer los riesgos más comunes del cibercrimen, lo cual ayudara a evitar grandes problemas y mitigar las vulnerabilidades, entre estos riesgos encontramos:

- **Tener equipos informáticos sin antivirus:** es importante que los sistemas informáticos tengan instalado y actualizado los antivirus para evitar presencia de virus informáticos, troyanos o gusanos.

- **No tener copias de seguridad:** las empresas contienen información relevante de sus productos, clientes o empleados como bases de datos o algún software para gestionar las actividades, es importante que realicen copias de seguridad periódicamente, las cuales además deben estar cifradas de lo contrario el riesgo a perder la información y no recuperarla genera un grave problema que afecta a toda la organización, incluso detiene el normal funcionamiento de las actividades de la empresa y su productividad. Las copias de seguridad deben realizarse correctamente porque en algunos casos se realizan copias de manera errónea y se tienen los mismos riesgos por ejemplo cuando se almacenan en los equipos informáticos los cuales pueden también afectarse y perder la información, en USB o discos duros externos que al estar conectados a los computadores podrían infectarse, por lo tanto, es recomendable realizar varias copias de seguridad en diferentes medios ya sean en la nube y en dispositivos de respaldo.

- **Abrir correos desconocidos:** evitar descargar archivos adjuntos desconocidos o abrir enlaces de procedencia sospechosa y no brindar información confidencial cuando los correos que se reciben dirigen a páginas que solicitan datos privados, los correos pueden contener virus o casos de phishing.

- **Abrir mensajes sospechosos en redes sociales**: algunas veces en las redes sociales llegan mensajes de desconocidos indicando ingresar a un enlace el cual puede contener virus o se la utiliza por los ciberdelincuentes para realizar alguna técnica de ingeniería social.

- **Introducir memorias USB o dispositivos en la computadora**: se debe analizar por un antivirus el dispositivo que se introduce antes de ser utilizado, ya que a pesar de ser útiles son introducidas en otros computadores que pueden estar infectados y contener virus, es recomendable enviar información de un sitio a otro por medios seguros como la red privada o programas en la nube.

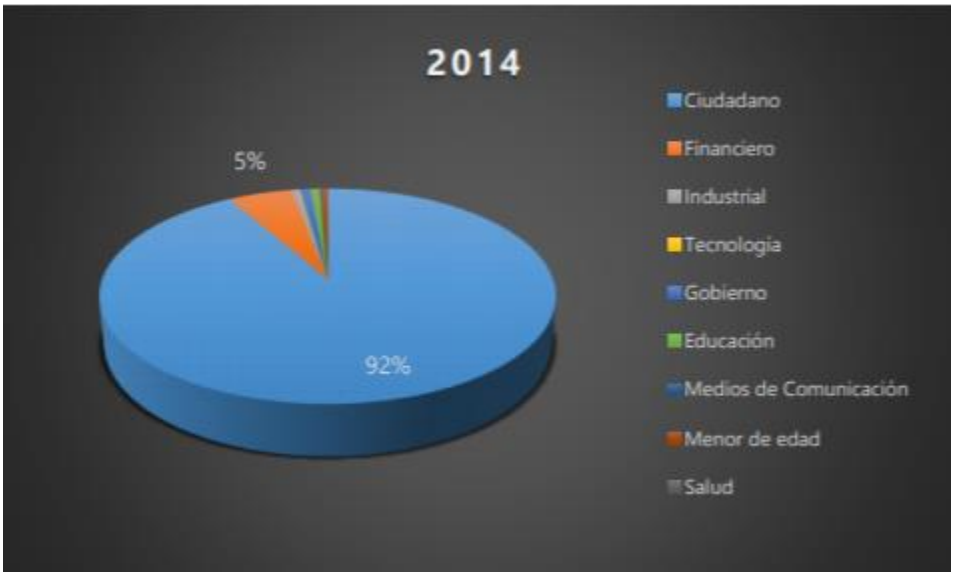
Smishing. Este delito informático utiliza mensajes de texto donde se solicita a la víctima comunicarse con un número o ingresar a una página web, el intruso puede suplantar el número de un conocido o de una entidad reconocida para generar confianza en la victima y así obtener información confidencial. Un caso de este tipo sucedió en el 2019 cuando clientes de Bancolombia recibían mensajes de este tipo (González, 2020).

Caracterización del Cibercrimen

Selección de víctimas

Figura 1

Selección de víctimas del cibercrimen en el año 2014



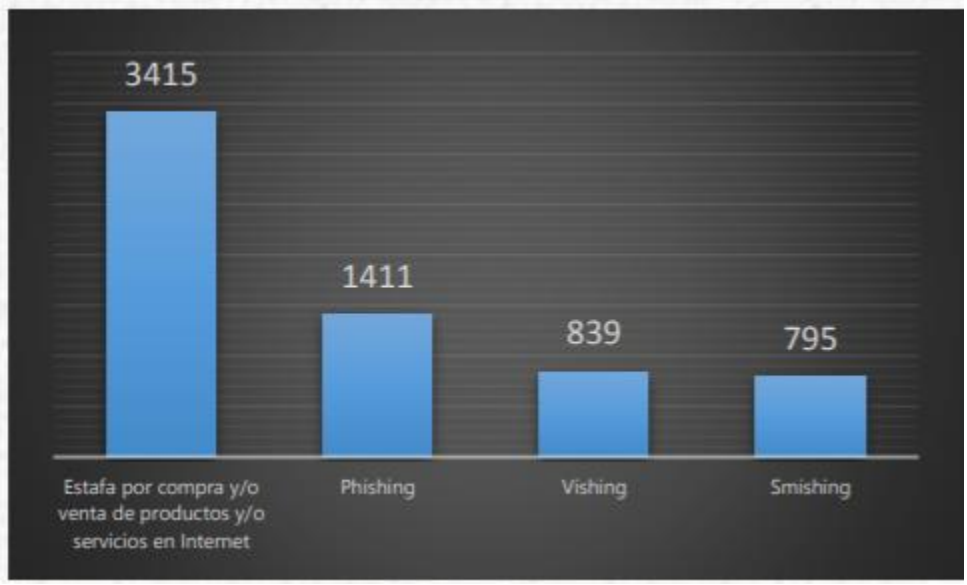
Nota. Las víctimas pasan del ciudadano común a las grandes empresas del sector público-privado, las cuales generan una mayor rentabilidad a la actividad criminal. Tomado de *Informe: Amenazas del Cibercrimen en Colombia 2016-2017* (p.2), por Policía Nacional, Dirección de Investigación Criminal e INTERPOL, 2017.

Nuevas plataformas de comercio electrónico utilizadas para estafar a través de *phishing*

Generalmente, el ciudadano del común es quien más accede a reportar eventos con un 66% de los incidentes, siendo una de las principales modalidades que afectan en Colombia las falsas ofertas publicadas en portales web e incluso reconocidas tiendas de comercio electrónico como mercadolibre.com, OLX.com, tucarro.com, etc.

Figura 2

Tipos de estafas



Nota. La figura ilustra los diferentes tipos de estafas presentadas en un espacio de tiempo específico. Tomado de *Informe: Amenazas del Cibercrimen en Colombia 2016-2017* (p.4), por Policía Nacional, Dirección de Investigación Criminal e INTERPOL, 2017.

Las estafas mencionadas se originan por el incumplimiento de algunas de las partes, bien sea en el envío o recibo de productos vendidos o comprados en las plataformas o en el cambio de las condiciones y calidad de estos. Cualquier producto puede ser utilizado como mecanismo de estafa virtual.

Servicios de Gobierno electrónico como vector de ataque para la distribución de *malware*

Ante la estrategia de Gobierno en Línea (*eGovernment*), que busca la generación de un estado más participativo, honesto, efectiva y transparente gracias a las TIC, es decir, que el Gobierno prestará los mejores servicios en línea al ciudadano, los cibercriminales identificaron que estas plataformas servirían para difundir *malware* y robar información a través de estos

servicios. El ingenio de los atacantes llegó incluso a utilizar falsos correos de instituciones la DIAN, Fiscalía General de la Nación y el SIMIT, para atraer la atención de las potenciales víctimas y lograr que dieran click sobre correos con asuntos sugestivos como “Invitación a pagar de manera urgente sus Obligaciones.zip”, el cual, al ser descargado por el usuario, ejecutaba un malware de nombre “TrojanWin32Xtratmzc” 17 que le permite al atacante ver todo lo que está ocurriendo en la máquina infectada.

Figura 3

Servicios de gobierno electrónico

Nota. La figura ilustra diferentes ejemplos de servicios de gobiernos electrónicos. Tomado de *Informe: Amenazas del Cibercrimen en Colombia 2016-2017* (p.5), por Policía Nacional, Dirección de Investigación Criminal e INTERPOL, 2017.

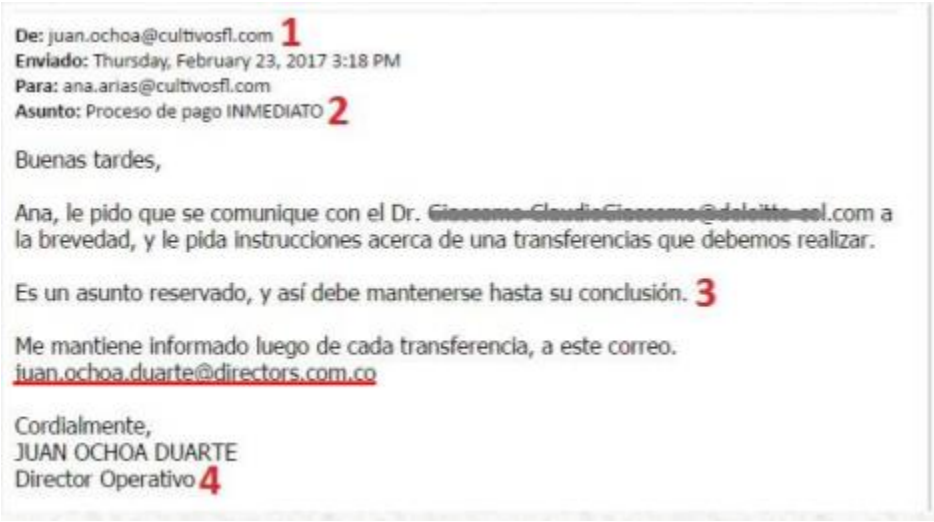
La participación de personas con acceso a información privilegiada o sensible de la víctima

a través de BEC. BEC (*Business Email Compromise*)

Esta se define como una estafa sofisticada, destinada a las empresas que trabajan con proveedores extranjeros y/o con empresas donde se llevan a cabo los pagos a través de transferencias electrónicas internacionales. La estafa compromete cuentas de correo electrónico de negocios legítimos a través de técnicas de ingeniería social o del acceso a la información para llevar a cabo transferencias no autorizadas de fondos. De acuerdo con un informe del FBI publicado en mayo de 2016, las víctimas perdieron $3mil millones de dólares a través de BEC. 20 Colombia no es ajena a esta modalidad, donde la principal característica es, el fraude CEO, en el que los ciberdelincuentes falsifican la dirección de correo ejecutivo de una organización, con el fin de iniciar una transferencia de fondos a sus propias cuentas. Se estima que por cada caso de BEC que afecte en Colombia, existe una pérdida de 130mil dólares (Federal Bureau of Investigation, 2016).

Figura 4

Business Email Compromise



Nota. La figura ilustra un caso particular de *Business Email Compromise*. Tomado de *Informe: Amenazas del Cibercrimen en Colombia 2016-2017* (p.6), por Policía Nacional, Dirección de

Investigación Criminal e INTERPOL, 2017.

A continuación, se mencionan diferentes aspectos a tener en cuenta para no ser víctima de esta estafa:

Un dominio de remitente falso. Los ciberdelincuentes suelen registrar un dominio similar a su destino.

Un asunto del correo electrónico urgente solicitando la transferencia de fondos inmediatos. Suelen utilizar líneas de asunto, que implican urgencia con respecto a las consultas sobre pagos o transferencias de fondos, tales como: Pago-Importante, Aviso de pago, Proceso de pago, Solicitud rápida, Fondo Recordatorio de pago, Solicitud de transferencia bancaria, etc.

Cuerpo del correo electrónico. En el fraude CEO, los estafadores hacen aparentar que se necesita urgentemente la transferencia de fondos y debe ser ejecutada tan pronto como sea posible. Además, se deben tener en cuenta los correos electrónicos mencionados, pidiendo la transferencia de fondos o la información de la transacción a una cuenta que es diferente al utilizado normalmente.

Posición del remitente del correo electrónico. Los cibercriminales que utilizan el fraude CEO normalmente se hacen pasar por alguien influyente en una organización.

Vinculación cada vez más frecuente de ciudadanos extranjeros en las organizaciones criminales con injerencia en Colombia. El fraude electrónico en cajeros automáticos ATM en Colombia ha sido uno de los vectores más explotados dentro de las entidades financieras, destacándose por su crecimiento en los últimos tiempos. Existen diversas técnicas con las cuales los ciberdelincuentes logran hacerse de una copia de la banda magnética o chip correspondiente a una tarjeta de crédito o débito, la cual es utilizada para consumar un hecho delictivo, realizando

compras o directamente retirando dinero de cuentas bancarias.

Presencia de usuarios colombianos en *Deep Web*. La *Deep Web* ya no es algo novedoso, de hecho, es un tema del que ha tomado fuerza desde hace un par de años. Pero en cierta forma, se ha convertido en tabú, porque sólo se habla de la gran cantidad de información de tipo malicioso que se puede encontrar allí. La *Deep Web* no es más que la parte de Internet que no ha sido indexada por algún tipo de buscador, por lo que la única forma de llegar a este tipo de información es conociendo la dirección exacta. Las razones por las cuales alguien podría no querer indexar su información abarcan un gran abanico de posibilidades, de las cuales no todas son necesariamente ilegales. De hecho, para una empresa puede ser importante que la página de acceso a algún servicio web no sea conocida en Internet. La red Tor (también conocida como nivel 4 de la *Deep Web*) se compone actualmente por aproximadamente 30.000 sitios web "*onion*" activos, lo cual la hace mucho más pequeña de lo que se pensaba anteriormente.

Figura 5

Sitio web "onion"

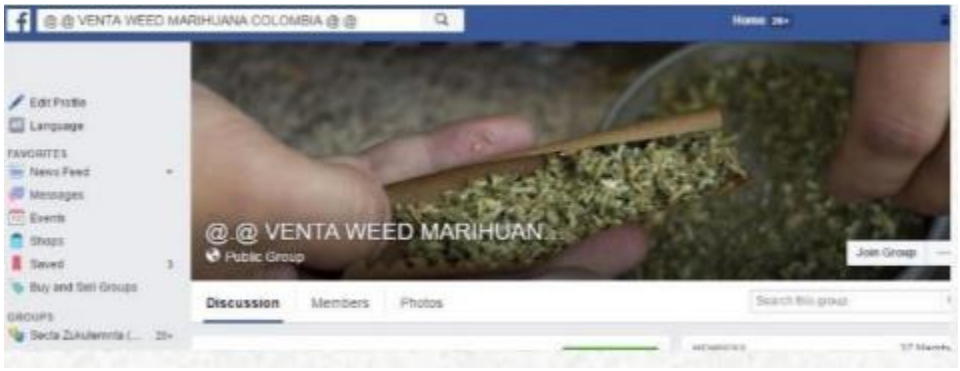
Nota. La figura ilustra un ejemplo de sitio web "*onion*" activo. Tomado de *Informe: Amenazas del Cibercrimen en Colombia 2016-2017* (p.8), por Policía Nacional, Dirección de Investigación

Criminal e INTERPOL, 2017.

En Colombia se han detectado más 280 páginas para la comercialización de drogas, accediendo a través de buscadores como Tor. Ofreciendo la droga sólo a ciudadanos extranjeros en el país, la transacción se realiza a través de correo electrónico cifrado, el pago a través de monedas virtuales y tanto el vendedor, como el comprador, no tendrían contacto físico para la entrega del producto ya que es dejado en un lugar que con posterioridad se le da a conocer al comprador por parte del vendedor.

Figura 6

Comercialización de drogas



Nota. La figura ilustra un ejemplo de página de comercialización de drogas. Tomado de *Informe: Amenazas del Cibercrimen en Colombia 2016-2017* (p.8), por Policía Nacional, Dirección de Investigación Criminal e INTERPOL, 2017.

De igual forma en redes sociales se han identificado grupos y perfiles que comercializan estupefacientes y drogas sintéticas en pequeñas cantidades, haciendo uso de plataformas de mensajería instantánea como Whatsapp, BBM, Telegram para concretar las formas de pagos de la compra y la entrega del producto, siendo estos últimos los medios de comunicación para la

negociación y las redes sociales para la oferta.

Uso del Internet como herramienta de amenazas e instigación a delinquir. El uso de internet va en aumento, es una herramienta fácil de usar y accesible para personas de todas las edades, donde son muchas las posibilidades que nos ofrece: conectarnos con amigos y familiares, acceder a información con fines educativos, entretenernos y aprender cosas nuevas; es una herramienta de la que se pueden obtener grandes beneficios. El cierre del primer trimestre del año 2016 arrojó un total de suscriptores a Internet en el país que alcanzó los 13.707.151, cifra compuesta por suscriptores a Internet fijo y móvil, lo que representa un índice de penetración del 28,1%, según el boletín trimestral del Ministerio TIC. Sin embargo, personas inescrupulosas han promovido un mal uso de internet, dando cabida a delitos y comportamientos indebidos como el Ciberbullying en todas sus formas: burlas, ridiculización, intimidación, amenazas, extorsión, etc. Así mismo la instigación a delinquir, apología al delito, suplantación de identidad, sextorsión, grooming, entre otros comportamientos inaceptables.

Uso de monedas virtuales como formas de pago. El fenómeno de las criptomonedas se ha vuelto la tendencia más revolucionaria en temas de *Ecomerce*. Actualmente las criptomonedas han alcanzado una variedad de más de 715 tipos diferentes, siendo el Bitcoin la más popular hasta el momento. Las criptomonedas no son emitidas ni reguladas por ningún banco o autoridad central. Por otra parte, tienen un valor muy inestable, lo que a muchos inversionistas aventureros les representa la posibilidad de una rentabilidad excepcional al comprar, cuando, por ejemplo, adquieren el Bitcoin si está a precios bajos y nuevamente revenderlos cuando los precios suban. Estas criptomonedas se convierten de información meramente lógica a unidades monetarias como es el peso colombiano, a través de los servicios *exchange*, que vienen a ser las casas de cambio de las monedas digitales. Otro aspecto importante para resaltar es la existencia de nuevos

servicios de *Outsoursing* para la gestión de Bitcoin, donde una persona compra Bitcoins a una empresa, esta le hace la conversión a la moneda local y automáticamente se va descontando del monedero del usuario (INFOLAFT, 2014).

Lo anterior, a través de la asignación de medios de pago tradicionales como es el caso de las tarjetas de crédito o débito. Es por esto por lo que las criptomonedas se convierten en una opción al alcance de los cibercriminales, para recolectar el pago de sus víctimas, sin ser reconocidos, al obviar la autoridad monetaria y permitir su uso directo entre pares.

Mapa de calor del Ciberdelito

Figura 7

Delito informático en Colombia

Nota. La figura ilustra la panorámica del delito informático en Colombia (mapa de calor). Tomado de *Informe: Amenazas del Cibercrimen en Colombia 2016-2017* (p.11), por Policía Nacional, Dirección de Investigación Criminal e INTERPOL, 2017.

Las principales ciudades con más reportes de incidentes informáticos son: Bogotá 9709, Medellín 691, Cali 475, Barranquilla 240 y Bucaramanga 12930 y las principales ciudades con mayores denuncias por Ley 1273 son: Bogotá 2607, Cali 1607, Medellín 998, Bucaramanga 594, Ibagué 448 y Barranquilla 398. Lo anterior, debido a que en estas ciudades se encuentra más del 75% de suscriptores de internet fijo dedicado y por mayor índice de habitantes por ciudad en el país (González, 2020).

Futuro del Cibercrimen

Internet de las cosas

La Internet de las Cosas (IoT, por sus siglas en inglés de *Internet of Things*) es un tema que se popularizó hace ya algunos años, y que desde el primer momento generó polémica y debate, sobre todo dentro de la comunidad de la Seguridad Informática, puesto que su aparición supuso (y supone) grandes y novedosos desafíos. El avance de la tecnología continúa expandiendo los límites y capacidades de dispositivos de este tipo; hay cada vez más aparatos que se conectan a Internet y son más accesibles, por lo que la superficie de ataques creció, algo que se evidenció en casos de campañas maliciosas que lograron comprometer a millones de usuarios en todo el mundo.

Es decir, durante los próximos años seguirá en aumento la cantidad de dispositivos que generan, almacenan e intercambian datos con los usuarios para mejorar su experiencia y simplificar muchas de las tareas que realizan. Existen 4.9 mil millones de dispositivos conectados a Internet y su número ascendió en 5 años hasta llegar a los 25 mil millones de dispositivos conectados a Internet para el 2020.

CONCLUSIONES

No obstante que en nuestro país las autoridades son responsables de generar consciencia en cuanto a la amenaza de los ataques Cibernéticos, Colombia en la actualidad es altamente vulnerable ante este riesgo, más aún desde que apareció la Pandemia del COVID-19. Es ineludible optimizar los análisis de la causa raíz que aminorarían el alto índice de ataques cibernéticos, estudio que ayudaría en la prevención, protección y detección temprana de los incidentes cibernéticos.

Es necesario sembrar políticas consolidadas de seguridad que preserven la información de todos los ciudadanos colombianos, de las diferentes empresas y redes, de manera tal que se congreguen normas, procedimientos y protocolos que redunden en proteger la información de los antes mencionados.

Nuestro país debe liderar estrategias que incluyan a todas las entidades públicas, privadas, empresas y hogares en general, buscando en todo momento una interacción que propicien proteger el ciberespacio nacional frente a agresiones potenciales. Por esto, es importante motivar y apoyar la exploración, mejora e invento de programas de enseñanza de cómo evitar ser víctima de cualquier ataque cibernético, así como favorecer toda buena práctica que redunde en menguar todo ataque cibernético a personas y empresas.

Finalmente es inevitable activar la práctica de denunciar todo delito cibernético que suceda ante las autoridades encargadas de analizar cuál fue el modus operandi y la causa que suscitó la materialización de este dolo, única manera de permitirle a nuestros mandos programar planes de acción que mitiguen la reproducción de este ilícito.

RECOMENDACIONES

A continuación, expongo las siguientes recomendaciones a la luz de lo abordado en el presente trabajo:

- Al Gobierno Nacional, instaurar políticas de seguridad asociadas con proteger la información, salvaguardar la privacidad y crear el uso adecuado de las redes.
- Al Gobierno Nacional, es importante considerar la protección de todos los equipos de cómputo, impresoras o aparatos inteligentes, pues igualmente pueden recibir ataques cibernéticos.
- Al Mintic, es importante considerar la protección de todos los equipos de cómputo, impresoras o aparatos inteligentes, pues igualmente pueden recibir ataques cibernéticos.
- Al Mintic, las políticas de confidencialidad garantizan la autenticidad de los datos.
- Al Mintic, las copias de seguridad reducen el impacto que genera un ataque informático, toda vez que pueden recuperarse más rápido.
- A las empresas en general, sin excepción alguna, deben tener instalados en todos sus equipos antivirus.
- A las empresas en general, las herramientas de seguridad advierten de posibles ataques exteriores en las diferentes redes locales.
- A las empresas en general, las claves por defecto deben ser cambiadas con regularidad, de esta forma es posible minimizar que curiosos accedan a las diferentes redes.
- A las empresas en general, las contraseñas complejas no fácil de descifrar, reduce la posibilidad de acceso por parte de la delincuencia.
- A las empresas en general, rechazar correos dudosos abrevia el robo de información.

Glosario

Amenaza. Puede ser definida como la posibilidad de que pueda llegar a ocurrir cualquier evento que atente contra la seguridad de la información, se genera una amenaza cuando se saca provecho de una vulnerabilidad en un sistema y puede generarse a través de ingeniería social o cuando no se da una correcta capacitación y concientización de los usuarios (Martínez, 2018).

Ataque. Se trata del aprovechamiento de las vulnerabilidades del software o hardware para ingresar con el objetivo de destruir, exponer, alterar, inhabilitar un sistema informático o la información que almacena o la red. Además, puede ser definido como un intento organizado por varias o una sola persona con el objetivo de causar daños a un sistema informático o una red. Un ataque usualmente puede ser provocado por delincuentes informáticos que realizan espionaje, suplantación de identidad entre otros (EDURED, s.f).

Botnet. Se refiere a un grupo de PC infectados y controlados por un atacante de manera remota. Por lo general un hacker o grupo de ellos crean un botnet utilizando un *malware*, el cual infecta a un grupo de computadores los cuales son parte del botnet llamados bots o zombies (Karpersky, s.f).

Denegación de servicio. El objetivo de este ataque es inhabilitar un sistema, una aplicación o una red bloqueando los servicios que ofrece, de esta manera impide que los usuarios legítimos puedan tener acceso, es causado por la saturación de los puertos con flujo de información, esto genera la sobrecarga delos servidores e imposibilita que presten los servicios (COMPUCHANNEL, 2018).

Exploit. Es un tipo de ataque que aprovecha las vulnerabilidades de aplicaciones, redes o hardware para obtener el control de un sistema o robar los datos que están en la red. Cuando en un software existen errores de programación los intrusos pueden utilizan estas debilidades para

controlar o infectar un sistema.

Grooming. Se trata de un engaño que realiza una persona adulta para ganarse la confianza de un menor de edad y abusar de ellos, puede presentarse personalmente o a través de internet generalmente se realiza en redes sociales. El acosador trata de apartar a la víctima de las personas que lo pueden apoyar como familiares o amigos para que se encuentra más vulnerable (Save the children, s.f).

Ransomware. Tipo de malware que bloquea archivos, sistemas informáticos o dispositivos y solicita un rescate para recuperar la información. Se pueden infectar a través de correos SPAM que contienen archivos adjuntos o enlaces a sitios web maliciosos. También se pueden infectar por ingresar a publicidad maliciosa (Karpersky, s.f y MALWAREBYTES, 2019).

Seguridad de la información. Medidas, herramientas y controles preventivos que deben tener en cuenta los individuos, organizaciones y tecnologías para proteger la información, con el fin de preservar la confidencialidad, autenticidad e integridad de los datos

Spam. Son correos que llegan a las cuentas sin haber sido solicitados y se envían automáticamente, se conoce también como correo basura, se utilizan para hacer publicidad o propagar el *malware* (SoftwareLab, 2020).

Spyware. Es una clase de malware que espía en el equipo informático o la red para tener acceso a información personal y confidencial. Se encarga de recolectar la información sobre las acciones que realiza un usuario con frecuencia, el historial de navegación o la información personal para enviarla a terceros sin que el usuario lo perciba. Un ejemplo de este tipo son los keyloggers los cuales se encargar de monitorizar las pulsaciones del teclado (Seguin, 2020).

Troyano. Programa malicioso que se presenta a los usuarios como software legítimo, se utiliza por los ciberdelincuentes para acceder a los sistemas, a través de ingeniería social engañan

a la víctima para que cargue y ejecute el troyano, cuando se activa los ciberdelincuentes pueden espiar, robar información o tener acceso al sistema por puertas traseras para eliminar, bloquear, modificar, copiar datos o interrumpir el rendimiento de los computadores o la red (Karpersky, s.f).

Virus informático. Son programas que alteran el funcionamiento de un sistema, sin que el usuario se percate de esto, generalmente infectan archivos para destruirlos o modificarlos, algunos causan daños graves y otros solo son molestos. Los virus pueden propagarse por medio de software y se pueden copiar de un archivo o computador a otro automáticamente (Torres, 2017 y Karspersky, s.f)).

Referencias

Amato, F., Castiglione, A., De Santo, A., Moscato, V., Picariello, A., Persia, F., Sperlí, G. (2018). Recognizing human behaviours in online social networks. Computers and Security, 74, 355-370. https://doi.org/10.1016/j.cose.2017.06.002

BBC Noticias. (2017). Un nuevo ciberataque de gran escala afecta a compañías e instituciones de todo el mundo.

COMPUCHANNEL (2018). ¿Qué es un ataque de denegación de servicios? Recuperado de: https://www.internetya.co/ataques-de-denegacion-de-servicios-ddos-un-riesgo-real/

Departamento de Justicia. Federal Bureau of investigation (2016). Business E-mail Compromise: The 3.1 Billion Dollar Scam. Recuperado de: https://www.ic3.gov/media/2016/160614.aspx

ECURED (s.f).Ataque informático. Recuperado de: https://www.ecured.cu/Ataque_inform%C3%A1tico

González (2020). Casos de estudio de cibercrimen en Colombia. Pasto, Nariño. Universidad Nacional Abierta y a Distancia.

INFOLAFT (2014). Lo que debe saber sobre el cibercrimen en Colombia. Recuperado de: https://www.infolaft.com/lo-que-debe-saber-sobre-el-cibercrimen-en-colombia/

Kaspersky (s.f). ¿Qué es un virus troyano? Recuperado de: https://www.kaspersky.es/resource-center/threats/trojans

Kaspersky (2013). ¿Qué es un botnet? Recuperado de: https://www.kaspersky.es/blog/que-es-un-botnet/755/

MALWAREBYTES (2019). Ransomware. Recuperado de:

https://es.malwarebytes.com/ransomware/

Martínez, E. (2018). Las diferentes amenazas de seguridad informática. Recuperado de: https://sites.google.com/site/lasamenazaslainformatica/

Publication Office of the European Union. EU Vocabularies. Recuperado de: https://op.europa.eu/en/web/eu-vocabularies/concept/-/resource?uri=http://publications.europa.eu/resource/authority/class-sum-leg/230806

Policía Nacional de Colombia, Dirección de Investigación Criminal e INTERPOL (2017). Informe: Amenazas del Cibercrimen en Colombia 2016-2017. Colombia. Recuperado de: https://www.caivirtual.policia.gov.co

Save the children (s.f). Grooming que es, como detectarlo y prevenirlo. Recuperado de: https://www.savethechildren.es/actualidad/grooming-que-es-como-detectarlo-y-prevenirlo

SoftwareLab (2020). ¿Qué es el SPAM? Recuperado de: https://softwarelab.org/es/que-es-spam/

Seguin, P. (2020). Spyware. Recuperado de: https://www.avast.com/es-es/c-spyware

Torres, G. (2017). ¿Qué es un virus informático? Recuperado de: https://www.avg.com/es/signal/what-is-a-computer-virus

Valle, M. (2016). El ransomware en cifras. Recuperado de: http://globbsecurity.com/ransomware-cifras-38969/